

Application No.: 09/632,933
Old Attorney's Docket No. 040070-692
New Attorney's Docket No. 0119-149
Page 2

Amendments to the Claims:

Please replace all prior versions, and listings of claims in the application with the following listing of claims.

Listing of claims

Claim 1 (currently amended): A method of generating an authentication ciphering offset (ACO) in a communication device, wherein the ACO is a number from which a ciphering key for the communication device is derived, and which is never communicated to any other communication device, the method comprising:

generating the ACO as a function of one or more parameters, wherein at least one of the one or more parameters is derived from earlier-computed values of the ACO.

Claim 2 (original): The method of claim 1, wherein the step of generating the ACO as a function of one or more parameters comprises generating a k th value, X_k from one or more of the parameters, and applying a commutative binary operation between X_k and a previous value, ACO_{k-1} .

Claim 3 (original): The method of claim 1, wherein the step of generating the ACO as a function of one or more parameters comprises:

generating a k th value of ACO as a running sum in accordance with:

$$ACO_k = X_k \oplus ACO_{k-1} = \sum_{i=1}^k X_i ,$$

wherein X_i is generated as a function of the one or more parameters excluding the at least one of the one or more parameters that is derived from earlier-computed values of the ACO.

Claim 4 (original): The method of claim 3, wherein the sum is a bitwise modulo-2 sum.

Claim 5 (original): The method of claim 4, wherein the bitwise modulo-2 sum is performed by means of a bitwise exclusive-OR (XOR) operation.

Application No.: 09/632,933
Old Attorney's Docket No. 040070-692
New Attorney's Docket No. 0119-149
Page 3

Claim 6 (currently amended): An apparatus for generating an authentication ciphering offset (ACO) in a communication device, wherein the ACO is a number from which a ciphering key for the communication device is derived, and which is never communicated to any other communication device, the apparatus comprising:

logic configured to generate the ACO as a function of one or more parameters, wherein at least one of the one or more parameters is derived from earlier-computed values of the ACO.

Claim 7 (original): The apparatus of claim 6, wherein the logic configured to generate the ACO as a function of one or more parameters comprises logic configured to generate a k th value, X_k from one or more of the parameters, and to apply a commutative binary operation between X_k and a previous value, ACO_{k-1} .

Claim 8 (original): The apparatus of claim 6, wherein the logic configured to generate the ACO as a function of one or more parameters comprises:

logic configured to generate a k th value of ACO as a running sum in accordance with:

$$ACO_k = X_k \oplus ACO_{k-1} = \sum_{i=1}^k X_i ,$$

wherein X_i is generated as a function of the one or more parameters excluding the at least one of the one or more parameters that is derived from earlier-computed values of the ACO.

Claim 9 (original): The apparatus of claim 8, wherein the logic configured to generate a k th value of ACO comprises logic configured to perform a bitwise modulo-2 sum.

Claim 10 (original): The apparatus of claim 9, wherein the logic configured to perform a bitwise modulo-2 sum comprises logic configured to performed a bitwise exclusive-OR (XOR) operation.

Claim 11 (original): The apparatus of claim 6, wherein the communication device includes a real-time device.

Application No.: 09/632,933
Old Attorney's Docket No. 040070-692
New Attorney's Docket No. 0119-149
Page 4

Claim 12 (original): The apparatus of claim 6, wherein the communication device includes a non-real-time device.